WHITEPAPER

FitMate

A TCM Safety Scanner and Consultation System Using Hybrid Rule-Based AI and WhatsApp Chatbot for Indonesian Consumers

Alvia Parausia Gionka[1] · Benedict Michael Pepper[2] · Lola Adelia Meidiyaratri[3]
Safrina Nur Maharani[4] · Rosselynd Elberta Christabel[5]

[134] Program Studi Farmasi · [2] Program Studi Teknik Informatika · [5] Program Studi Pendidikan Bahasa Mandarin
Universitas Ma Chung, Malang · PKM-KC 2026 · April 2026

Contact: 612410009@student.machung.ac.id

Executive Summary

Indonesia's growing consumption of Traditional Chinese Medicine (TCM) products operates largely without adequate consumer safety infrastructure. The majority of commercially available TCM labels are written in Mandarin, a script inaccessible to approximately 97% of the Indonesian population. Compounding this, Indonesia's national drug regulator (BPOM) identified 53 traditional medicine products containing illicit pharmaceutical chemicals in 2021, and a 2025 cyber patrol of online marketplaces flagged approximately 2,000,000 non-compliant herbal products, predominantly imported from China.

FitMate addresses this gap with a Progressive Web App (PWA) and WhatsApp chatbot that enables any Indonesian smartphone user to scan a TCM product label, extract and translate Mandarin ingredient text using a multimodal large language model (LLM), and receive a pharmacist-validated safety verdict in seconds. A strict hybrid architecture ensures that all safety determinations are produced exclusively by rule-based database logic, eliminating LLM hallucination from medical outputs while retaining the conversational quality of AI-generated responses. A functional prototype has been deployed and validated by pharmacy practitioners.

1. The Problem

Three compounding factors create Indonesia's TCM safety gap.

Language inaccessibility. TCM product labels distributed in Indonesia are predominantly printed in Mandarin. Without readable ingredient information, consumers cannot assess toxicity risks, contraindications, or interactions with existing medications (Nurhalisa et al., 2024).

Unsupervised self-medication. Consumers routinely use herbal products without knowledge of safe dosage limits or potential drug interactions, operating under the misconception that natural products carry no risk. Unsupervised self-medication remains a documented and growing phenomenon among productive-age Indonesians (Ghaznawi et al., 2025; Esti et al., 2025).

Proliferation of unsafe and unregistered products. BPOM's 2021 Public Warning identified 53 traditional medicine products containing illicit pharmaceutical chemicals (bahan kimia obat, BKO), including ephedrine, pseudoephedrine, sildenafil, tadalafil, and dexamethasone. Approximately 11.3% of products banned in 2021 remained available on e-commerce platforms through 2026. BPOM's 2025 cyber patrol found 197,725 non-compliant product links across online marketplaces, with illegal herbal products ranking as the second-largest category of violations.

Existing digital health tools address general health consultation, medication reminders, or wellness education. None offer TCM-specific ingredient safety scanning with pharmacist-validated toxicity data delivered in a zero-installation format appropriate to Indonesia's messaging infrastructure.

2. System Architecture

2.1 Overview

FitMate consists of three integrated subsystems: a React.js/Next.js Progressive Web App providing camera access, image capture, and real-time toxicity visualization; a Python FastAPI backend orchestrating OCR processing, database lookup, fuzzy ingredient matching, and WhatsApp webhook handling; and a Twilio-integrated WhatsApp bot providing conversational TCM safety consultation, accessible independently of the web scanner.

Both interaction paths share a single backend API and processing layer. Safety verdicts are determined exclusively by the rule-based safety service; the LLM has no involvement in producing or modifying them.

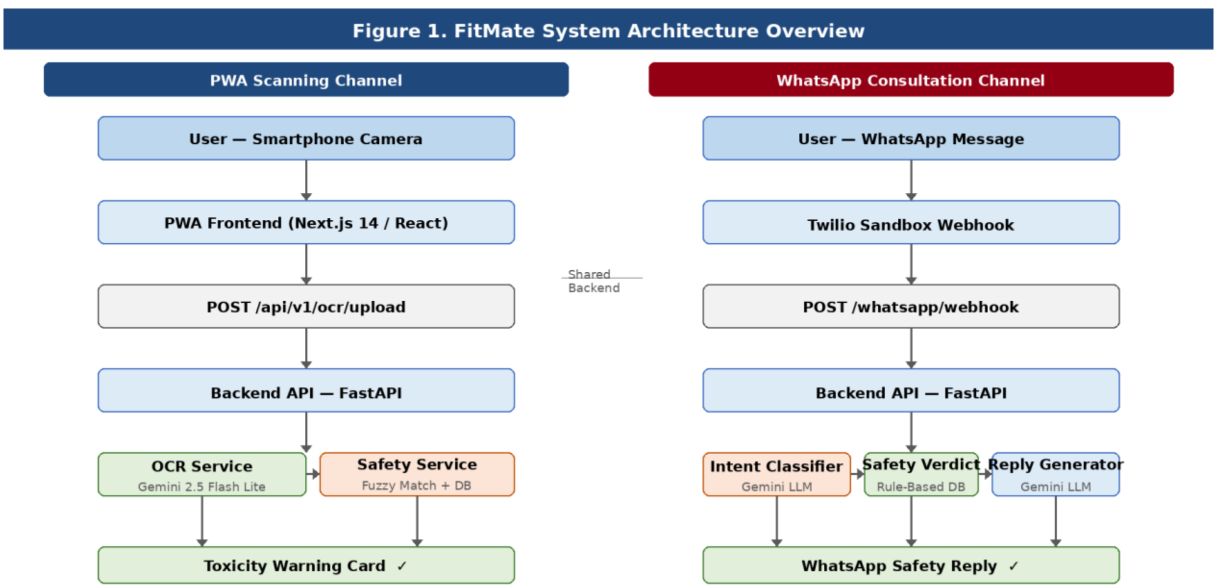

Figure 1. FitMate system architecture: web scanner path (left) and WhatsApp consultation path (right) share a common backend API. The safety verdict is determined solely by the rule-based service layer.

2.2 Hybrid AI Architecture

Core design principle: The LLM classifies intent, extracts ingredient names, and generates conversational replies. It never determines safety verdicts. All safety outputs are produced by deterministic rule-based database lookups traceable to pharmacist-validated entries.

This functional partition satisfies three requirements simultaneously. First, it eliminates LLM hallucination from the medical output layer: a false 'safe' verdict produced by a probabilistic language model would constitute a direct patient safety risk. Second, it enables systematic pharmacist review of the underlying data rather than AI output auditing, since the safety logic is explicit and traceable. Third, it preserves conversational quality for informational queries, where the LLM can draw on the database's contraindication descriptions to generate empathetic, context-aware replies.

For ingredient safety inquiries, the processing sequence is: (1) intent classification by LLM, (2) ingredient name normalization by LLM, (3) fuzzy database lookup by the rule-based service, (4) verdict retrieval as a constant string value ('safe', 'toxic', or 'not found'), and (5) reply generation by LLM, which is instructed to acknowledge the verdict faithfully and may not contradict it.

2.3 OCR and Ingredient Extraction

Label image processing uses Gemini 3.1 Flash Lite in multimodal mode, accessed through the OpenRouter API. Unlike conventional OCR pipelines that treat label reading as character-level text extraction, the multimodal LLM approach applies semantic understanding of pharmaceutical Chinese to produce structured ingredient data.

The system prompt instructs the model to identify all ingredient names in the image, return both the Mandarin form and the most common Indonesian or Pinyin transliteration for each ingredient, ignore non-ingredient text (branding, dosage instructions, registration numbers), and return structured JSON for downstream database lookup. This approach handles challenging label conditions that defeat conventional OCR: partially obscured text, metallic foil packaging, ultra-small character sizes, and traditional script variants (fantiezi).

2.4 Ingredient Safety Matching

Extracted ingredient names are matched against the MongoDB knowledge base using fuzzy string matching (thefuzz library, token_set_ratio method). Each name is compared against five variant fields per database entry: Indonesian name, Mandarin characters, Pinyin, English common name, and Latin botanical name. A minimum match threshold of 68 out of 100 is required for acceptance.

Below this threshold, the ingredient is classified as 'not found' and the system explicitly acknowledges uncertainty rather than defaulting to a 'safe' assumption. This conservative behavior is intentional: a false-negative match producing an incorrect 'safe' verdict carries direct patient safety consequences. The intent classifier's normalization step further improves match accuracy by translating foreign-language ingredient names (German, Dutch, Latin) to standard Indonesian, English, or Pinyin equivalents before matching.

3. Pharmacist-Validated Knowledge Base

The TCM ingredient knowledge base was constructed through a three-stage pipeline: data collection from SymMap, TCMID (Traditional Chinese Medicine Integrated Database), and BPOM Public Warning Lists; pharmacist review by three licensed pharmacy students under faculty supervision; and structured seeding into MongoDB.

Pharmacist reviewers assessed the accuracy of toxicity classifications, the currency of contraindication information against pharmacological literature, the accuracy of Indonesian-language descriptions, and the correctness of Mandarin, Pinyin, and Latin name variants. The resulting database contains 103 entries covering the most commonly consumed TCM products and ingredients in the Indonesian market.

Category	***Entries***	***Coverage Rationale***
TCM patent medicines and herbal supplements	*50*	*Top 50 consumed products in the Indonesian market*
Culinary herbs and medicinal cooking ingredients (ciakpo)	*50*	*Dual-use herbs commonly found in TCM formulations*
Toxic or BPOM-flagged substances	*13*	*Aristolochic acid, hepatotoxic alkaloids, pregnancy contraindications*
TOTAL	103	*v1.1 prototype database*

Table 1. Database coverage summary by ingredient category. The 13 toxic entries include entries that also appear in the 100 main categories.

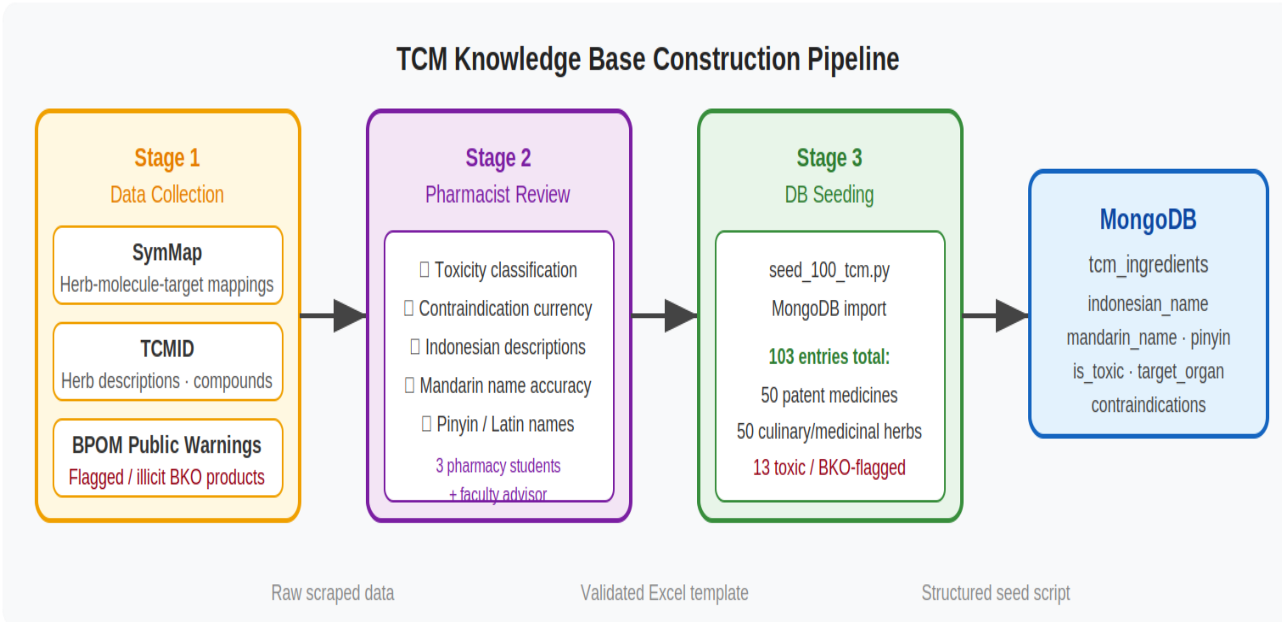

Figure 2. Knowledge base construction pipeline: data collection from SymMap, TCMID, and BPOM sources; pharmacist review by pharmacy students under faculty supervision; structured seeding into MongoDB.

Each database entry stores the primary Indonesian display name, Mandarin characters for OCR matching, Pinyin romanization, English common name, Latin botanical name, a boolean toxicity verdict field (is_toxic) that exclusively drives the rule-based safety determination, a toxicity severity classification (mild/moderate/severe), target organ system, free-text contraindication description, and a plain-language informational description.

4. WhatsApp Consultation Bot

The WhatsApp bot operates as a standalone consultation channel accessible without the web scanner. Users can query safety information by typing ingredient names or natural language questions through any WhatsApp-enabled device, with no application installation or account registration required. WhatsApp reaches over 90% of Indonesian smartphone users, making it the most accessible delivery channel for this population.

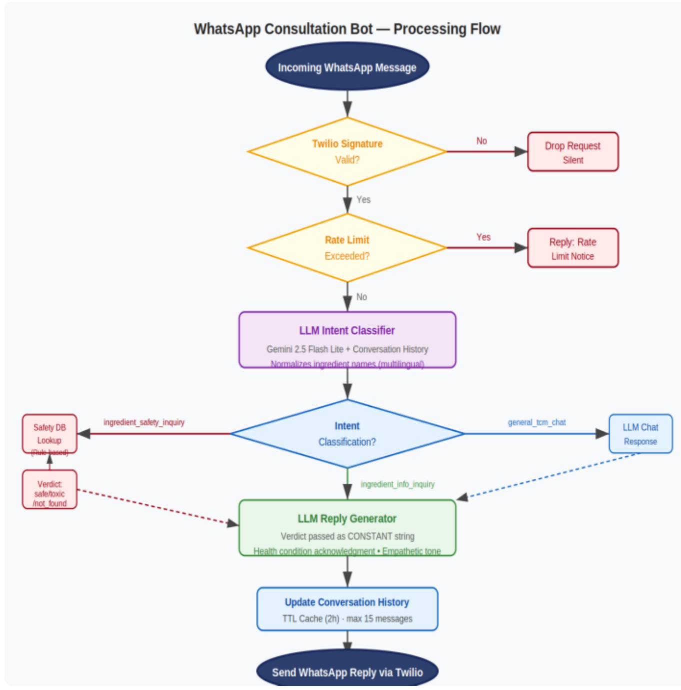

Figure 3. WhatsApp consultation bot processing flow: incoming message through security validation, rate limiting, intent classification, rule-based safety verdict determination, LLM reply generation, and conversation history update.

Incoming messages are classified into one of three intent categories by the LLM: an ingredient safety inquiry (asking whether an ingredient is safe, toxic, or suitable for a health condition), an ingredient information inquiry (asking what an ingredient is or its medicinal uses), or general TCM conversation (greetings, general health questions). Safety inquiries route exclusively through the rule-based database layer; informational inquiries draw on the database's description fields; general conversation uses the LLM directly.

Health condition acknowledgment. A key feature is the explicit acknowledgment of user-stated health conditions in safety replies. When users mention conditions such as diabetes, pregnancy, hypertension, or kidney disease, the reply generation prompt instructs the LLM to name the condition explicitly and draw on the database's contraindication field to provide condition-appropriate context, while attributing this guidance to the database rather than AI-generated medical opinion.

Conversation memory. Per-user conversation history is maintained in a TTL cache (2-hour session window, maximum 15 messages) enabling multi-turn consultation, including reference resolution across turns.

Multi-ingredient batch lookup. When a message contains comma-separated ingredient names (as produced by a label-scanning scenario), the system executes parallel database lookups and returns a consolidated safety card. Each ingredient is independently classified; a safe result for one ingredient does not mask a toxic classification for another.

5. Implementation

The frontend is built on Next.js 14 with Tailwind CSS, deployed as a Progressive Web App on Vercel for cross-platform mobile access without app store requirements. The backend uses Python 3.11 with FastAPI for asynchronous processing and Pydantic data validation, deployed on an AWS EC2 instance to support HTTPS for Twilio webhook callbacks. MongoDB serves as the primary data store for its flexible schema suited to evolving TCM data structures. WhatsApp integration uses the Twilio Sandbox for rapid deployment without requiring Meta Business verification.

5.1 Security Controls

All incoming WhatsApp webhook requests are validated against the X-Twilio-Signature header using HMAC-SHA1; requests failing validation are silently dropped. The OCR endpoint is rate-limited to 5 requests per minute per IP address; the WhatsApp bot applies per-phone-number rate limiting at 20 messages per 10 minutes. All service credentials are stored in environment variables and excluded from version control. API responses include X-Content-Type-Options, X-Frame-Options, and Referrer-Policy headers via custom FastAPI middleware.

5.2 User Interface

The PWA follows a 'Modern Apothecary' design concept using a 60-25-10-5 colour ratio, with Imperial Red (#930014) reserved exclusively for toxic ingredient warnings. Typography uses Merriweather for headings, Inter for body text, and Noto Sans SC for Chinese character display. The interface is designed for glanceability: a user should be able to determine whether a scanned product is safe or contains a flagged ingredient within 2 seconds of receiving the scan result.

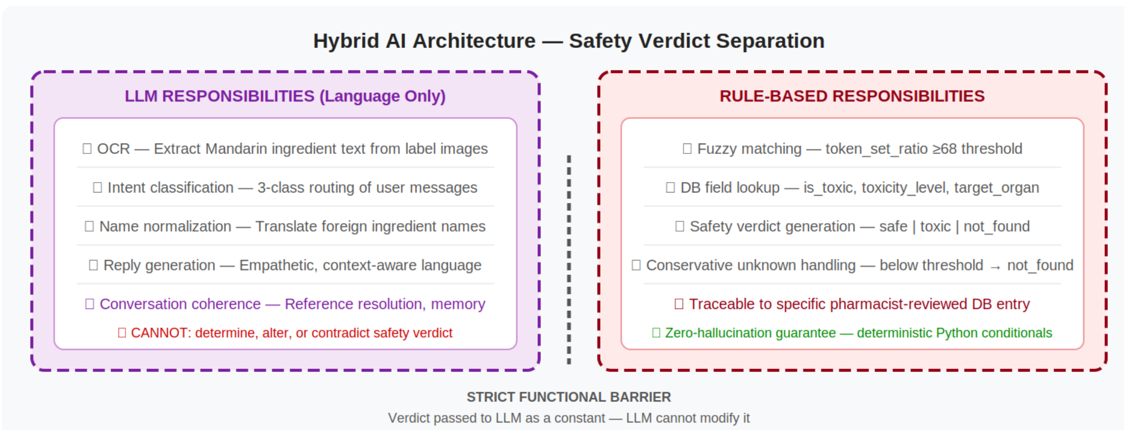

Figure 4. Hybrid AI architecture separation: LLM responsibilities (left) are limited to language tasks; rule-based responsibilities (right) handle all safety determination. A strict functional barrier prevents the LLM from modifying or contradicting the safety verdict.

6. Testing and Evaluation

The OCR pipeline was evaluated against 25 TCM product label photographs captured under varied conditions, including outdoor lighting, low-contrast backgrounds, metallic packaging, and angled shots. The target standard was 85% or greater ingredient extraction accuracy, consistent with the system's design requirement (SCAN-04). The hybrid rule-based architecture was verified by code review and test case execution to confirm that no tested scenario produced an LLM-modified safety verdict.

All database entries and system output formats were reviewed by pharmacy student team members and a faculty pharmacist advisor. Validation specifically addressed accuracy of toxicity classifications, correctness of contraindication descriptions, appropriate scope of the medical disclaimer, and whether any LLM-generated reply language could be interpreted as prescriptive medical advice. No medically misleading output was identified in any tested scenario.

User Acceptance Testing (UAT) with 15-20 members of the general public evaluates: scanning a provided TCM product label, reviewing the safety result, conducting a multi-turn WhatsApp consultation that includes stating a health condition, and reviewing a multi-ingredient label by typing an ingredient list into the bot directly. Usability is assessed on ease of use, clarity of safety information, perceived trustworthiness, and willingness to use the system before purchasing a TCM product.

7. Results

The end-to-end pipeline from label photograph to structured safety output was successfully implemented and verified. Gemini 3.1 Flash Lite produces structured ingredient extraction from TCM labels, including correct identification of ingredients from stylized and low-contrast typography that defeats conventional character-level OCR.

Following iteration on the chatbot system prompts, the bot demonstrates four measurable improvements over naive LLM-based consultation: explicit naming of user-stated health conditions with condition-appropriate context drawn from the database contraindication field; successful normalization and matching of foreign-language ingredient names (German, Dutch, Latin) that appear on imported TCM products; coherent multi-turn conversation with reference resolution across turns; and a complete standalone consultation experience requiring no prior use of the web scanner.

7.1 Identified Limitations

Database coverage is the primary constraint of the current prototype. The 103-ingredient database covers a minority of ingredients present in the full Indonesian TCM market; queries for unlisted ingredients return a 'not found' response, which is the correct conservative behavior but limits practical utility for less common products.

In-memory conversation storage resets on server restart, which in a development environment with hot-reload causes repeated welcome messages when code changes trigger restarts. Fuzzy matching performs well for transliteration variants but fails on semantic similarity queries; this is partially mitigated by the LLM normalization step but remains a ceiling on matching accuracy for novel ingredient names.

8. Development Roadmap

Four near-term enhancements are prioritized for the next development phase. First, database expansion to 500 or more entries via the existing BPOM/SymMap/TCMID pipeline, concurrent with converting the free-text contraindications field to a structured contraindicated_conditions array for deterministic conditional matching. Second, multilingual semantic embedding search using the paraphrase-multilingual-MiniLM-L12-v2 model to replace lexical fuzzy matching, enabling accurate cross-language retrieval and semantic similarity queries (for example, surfacing aristolochic acid entries from a query about 'herbs associated with kidney failure'). Third, a persistent user health profile keyed by WhatsApp phone number, enabling automatic application of condition-specific safety logic across sessions without requiring users to re-state their health context. Fourth, a drug-herb interaction module addressing clinically documented interactions between TCM ingredients and conventional pharmaceuticals, including Danshen with warfarin, licorice root with corticosteroids, and ginkgo biloba with anticoagulants and SSRIs.

9. Conclusion

FitMate demonstrates that a strict functional separation between LLM-mediated language tasks and rule-based medical determination is achievable in a production-grade mobile system, and that this architecture resolves the core tension between conversational usability and medical reliability in AI health tools.

The system makes three concrete contributions. It provides a pharmacist-validated TCM safety knowledge base covering 103 of the most commonly consumed TCM ingredients in Indonesia, with a data pipeline supporting systematic expansion from BPOM, SymMap, and TCMID sources. It delivers a WhatsApp-native consultation interface that functions as a complete standalone safety channel accessible to any Indonesian smartphone user without installation or registration. And it establishes a verified hybrid architecture in which all safety verdicts are traceable to specific pharmacist-validated database entries, enabling practitioner review of the underlying data rather than AI output auditing.

The documented scale of unsafe TCM product circulation in Indonesia (BPOM, 2021; 2025; 2026) indicates a public health gap that self-regulatory and registration-based approaches have not closed. FitMate's approach of embedding safety screening within Indonesia's existing messaging infrastructure represents a direction for accessible, practitioner-supervised consumer protection at scale.

References

Badan Pengawas Obat dan Makanan. (2021). Public Warning Obat Tradisional, Suplemen Kesehatan, dan Kosmetika Mengandung Bahan Kimia Obat/Bahan Dilarang Tahun 2021. Jakarta: BPOM.

Badan Pengawas Obat dan Makanan. (2025). Indonesia dan Tiongkok Perkuat Sinergi Budaya dan Ilmu Pengetahuan dalam Pengembangan Obat Tradisional. Jakarta: BPOM.

Badan Pengawas Obat dan Makanan. (2026). Hasil Patroli Siber Marketplace 2025: Temuan Produk Obat Tidak Sesuai Ketentuan. Jakarta: BPOM.

Esti, N., Rahmawati, D., & Prasetyo, A. (2025). Perilaku unsupervised self-medication pada kelompok usia produktif di Indonesia. Jurnal Kesehatan Masyarakat Nasional, 20(2), 101-109.

Fadhilah, R., Maulani, M. R., Resdiana, W., & Hamidin, D. (2024). Integrasi fitur Chatbot dalam aplikasi edukasi kesehatan dan kebugaran menggunakan algoritma neural network. Jurnal Kecerdasan Buatan dan Teknologi Informasi, 3(3), 125-135.

Ghaznawi, U. U., Akhtar, L., Rehmat, A., Younas, I., & Ullah, S. (2025). Assessment of multivitamin usage and factors affecting lifestyle. BMC Nutrition, 11, 27.

Kurniasih, H., Winarso, P., & Sartika, L. (2024). Pengembangan aplikasi bot WhatsApp pengingat minum obat untuk meningkatkan kepatuhan minum obat pada ibu hamil dengan hipertensi. Seminar Nasional Keperawatan, 22, 162-166.

Nurhalisa, F., et al. (2024). Traditional Chinese Medicine sebagai warisan budaya dan praktik kesehatan etnis Tionghoa di Indonesia. Jurnal Sejarah dan Kebudayaan, 12(1).

Pantan, F. (2023). Pemanfaatan Chatbot berbasis kecerdasan buatan dalam layanan konsultasi digital. Jurnal Teknologi Informasi, 8(2).

Rahmasiah, R., Roni, R., Hadi, S., & Termia, M. (2023). Gambaran pengetahuan masyarakat tentang peredaran sediaan farmasi obat tradisional non BPOM di Kelurahan Rijang Pittu Kabupaten Sidrap. Marendeng Journal, 7(2), 49-57. https://doi.org/10.58554/jkm

Wahab, B., Apriana, A., & Silitonga, D. (2025). Perancangan sistem konsultasi kesehatan online berbasis website guna meningkatkan efisiensi dan efektivitas pelayanan kesehatan pada UPTD Puskesmas Tiga Balata tahun 2025. Jurnal Penelitian Kesmasy, 7(2).

World Health Organization. (2019). WHO Global Report on Traditional and Complementary Medicine 2019. Geneva: WHO.

Acknowledgments. The authors thank the faculty pharmacist advisor at Universitas Ma Chung for expert review of the TCM safety knowledge base. This work was supported by the PKM-KC (Program Kreativitas Mahasiswa, Karsa Cipta) scheme of Indonesia's Ministry of Education, Culture, Research, and Technology (Kemendikbudristek) through the Simbelmawa platform.